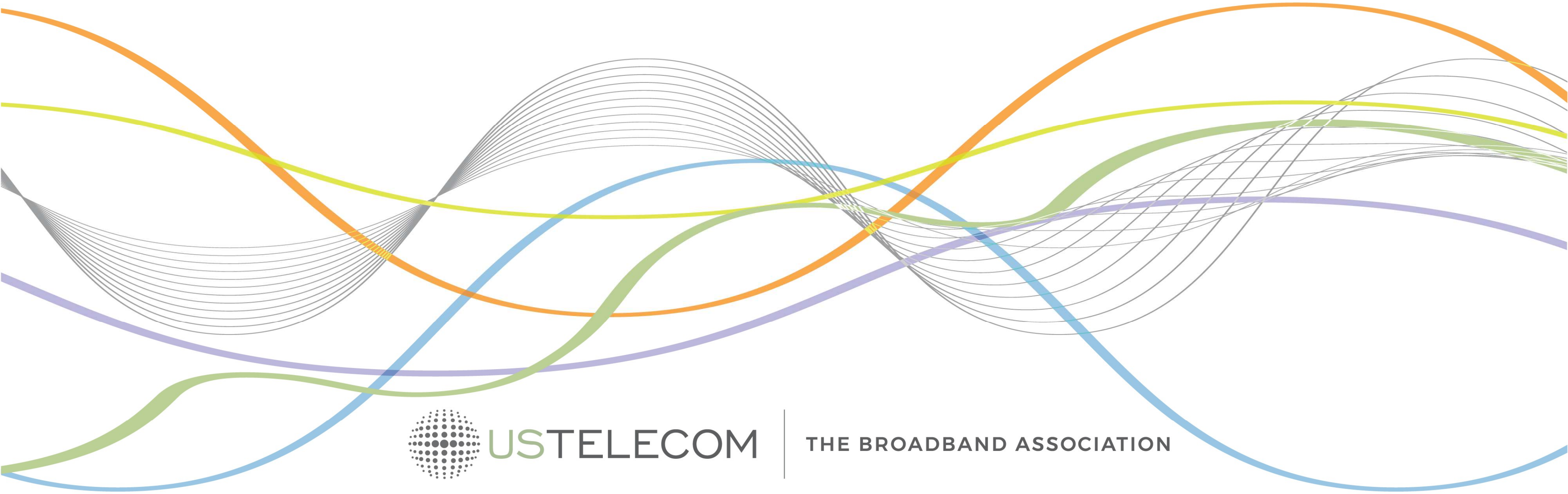
Mitigating Robocalls Best Practices

November 2020

INDUSTRY TRACEBACK GROUP



USTELECOM | THE BROADBAND ASSOCIATION

Overview

- Providers ask us: What should we be doing to prevent illegal robocalls via our platform?

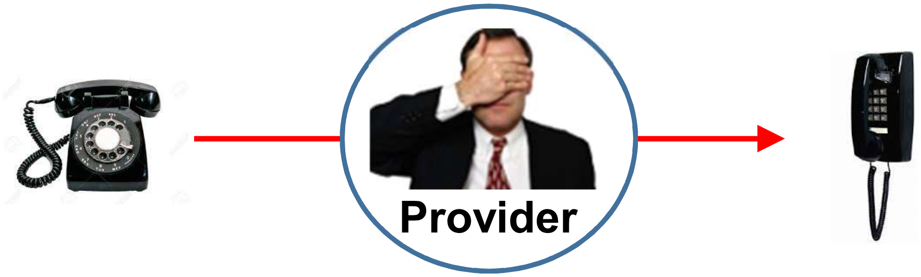
- For this webinar, we have collected best practices from multiple sources:
  - Processes successfully implemented by other providers
  - Practices recommended by US State Attorneys General
  - Practices published by the North American Numbering Council
  - Settlements reached with enforcement agencies
  - Suggestions from other stakeholders based on analyses of robocaller behavior

- We have divided the session into three sections:
  - Know the Rules
  - Know Your Customer
  - Know Your Traffic

- Message us with your questions during the session
- We'll have dedicated Q&A time at the end as well

Know Why You Should Care

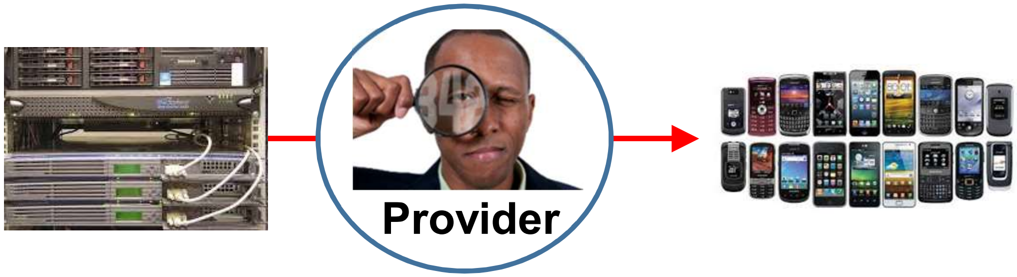
- **BEFORE: Providers just passed calls through**



Provider

Enforcement focused on the Caller.

- **NOW: Providers share responsibility for stopping and preventing illegal robocalls**



Provider

- New U.S. laws and enforcement also make providers responsible for calling violations
- There is momentum in the regulatory framework to ensuring that downstream providers only take traffic from trusted & compliant upstream providers

Know the Rules

- There are extensive rules that apply to calls directed to USA telephone numbers
  - Every provider sending calls to USA should be familiar with these rules
  - Those providers should ensure that their callers know and understand the rules
- Telephone Consumer Protection Act (Federal Communications Commission – FCC)
- Telemarketing Sales Rule (Federal Trade Commission – FTC)
- Truth-in-Caller-ID (FCC)
- TRACED Act (FCC)
- State-Specific Calling Rules (also have authority under TCPA)
- Laws covering Fraud and Harassment (Federal & State)
- Provider Terms of Service and Acceptable Use Policies (Provider-Specific)
- Penalties for violations include:
  - Fines and imprisonment
  - Downstream provider refusal to accept traffic
- It is the responsibility of providers and callers to know and comply – qualified legal help may be required

Most-Frequently Violated Rules

- AUTOMATED calls to wireless and do-not-call numbers are generally prohibited
  - Playing a pre-recorded message, or
  - Using an artificial voice, or
  - Placed via an autodialer

- All automated messages (even when placed with consent from the called party) must include:
  - The name of the entity responsible for the call
  - A valid call-back number (toll-free if a telemarketing message left in voice-mail)
  - An automated opt-out capability for telemarketing calls

- Caller-ID must not mis-use others' numbers

- All providers should cooperate with traceback
  - Respond to all traceback requests with the identity of the upstream source of the call
  - Take effective steps to address illegal traffic
  - Insist that upstream call sources comply

Fraudster Shopping List

- Many simultaneous calls
- High calls-per-minute
- Unrestricted Caller-ID
- No penalty for short-duration calls
- Anonymous sign-up
- Low per-minute rate

Know Your Customer

How well you must know your customer depends on the service they will be allowed to access:

- Volume of calls they can place
    - Calls per second
    - Number of concurrent calls

- Caller-ID values they can use;
    - # assigned by you
    - #'s you have verified
    - non-US #'s
    - any # including US

- Enable the customer ONLY for the type of traffic you expect them to use

Know Your Customer

For each customer, obtain, review and verify:

- Full business name and government registration information
- Contact names, titles, direct-dial telephone numbers, email addresses and physical addresses
- Description of business
- Description of calling traffic (call volumes, durations, nature of calls)
- Web site consistent with the above
- Complete knowledge and compliance with calling rules
- Consent to disclose all details if questions arise regarding potential illegal calling

For service provider customers, also confirm:

- Provider is aware of traceback process and will respond promptly to all requests
- Provider will ensure all upstream sources are compliant

Implementing Know Your Customer

- Questionnaire (example)
- Vetting (potentially by a third-party specialist)
- No anonymous sign-ups
- Contractual requirements

- Frequent issues we see:
  - Inconsistent names
  - Inconsistent addresses / phone numbers
  - Incomplete web sites
  - @gmail.com and other “throw-away” addresses

- If in doubt:
  - DENY service, or
  - LIMIT volume; RESTRICT allowable caller-ID values

Provider Caller-ID Rules – Safe or Risky?

Caller-ID Value is a number assigned to the Caller by the Provider.	**SAFEST –** track number assignments & purpose
Caller-ID Value is on a list that Provider has verified the Caller has permission to use.	**WORKABLE –** if verification is solid
+1 USA Caller-ID not permitted unless Customer is confirmed to be in USA.	**RISKY –** watch for fake USA addresses – but still better than no checking! ⚠
Caller-ID value is not checked.	**DANGEROUS –** very easy to abuse ⚠

Know Your Traffic

- Implement an on-going **traffic monitoring program** to identify potential illegal calling
  - Assess daily traffic on a customer-by-customer basis
  - Ensure traffic patterns are consistent with customer’s profile

- **Key metrics to watch:**
  - Average Call Duration (calls shorter than 6, 18, 30, 60 seconds)
  - Trends in daily call volume
  - Answer Seizure Ratio (fraction of calls answered)
  - Unique Caller-ID values (ratio of total calls to unique CLID’s)

- **Traffic patterns** inconsistent with conversational calling should trigger an investigation
  - Engage with traffic source to obtain definitive explanation for suspicious traffic

How Traceback Fits

- When you get a traceback notice, it means there is a problem with your efforts to PREVENT illegal robocalls
- Usually, one traceback is representative of a large volume of similar calls
- Where there's smoke, there's typically fire

How Traceback Fits

In response to a traceback notice:

- **Respond promptly** with details regarding the source of the call (who sent it to you)
- Initiate a **review of that source**
  - Revisit the know-your-customer details that you have on file, or launch a new KYC effort
  - Audit recent traffic metrics (see earlier best practices)
- Read the **Campaign description** and listen to the audio (usually provided in the TB Portal)
  - Decide for yourself if the call is compliant with all regulations
- **RAPIDLY** confer with your customer and/or take steps to **stop ALL illegal calls**
  - Note that blocking a single ANI rarely addresses the root cause
- Submit **COMMENTS** in the TB Portal so that the record of the incident is complete

Know What Happens When Things Go Wrong

Providers that fail to take sufficient steps to mitigate and prevent illegal robocalls enable and encourage billions of illegal robocalls that plague the U.S. telephone network and ultimately consumers

- Robocalls are beyond annoyances – victims are defrauded of millions of dollars per year, including those most vulnerable among us

- Illegal robocalls also can cause safety of life concerns (*e.g.*, a TDoS attack to a hospital or police office)

Know What Happens When Things Go Wrong

USA Regulators and Enforcers are putting additional burdens on providers:

- Enforcement with multi-million-dollar penalties and forced exit from the market
  - FCC, FTC, DOJ, and state AGs all are intent in bringing enforcement actions against enabling providers
- Downstream providers blocking *all* calls from a provider if that provider is identified by the FCC as a “bad actor”
- Starting in June, most U.S. providers will need to certify to the FCC that they have implemented a “robocall mitigation program”
  - Downstream providers then will be prohibited from accepting traffic from a provider that is not in the FCC’s Robocall Mitigation Database
  - FCC will impose prescriptive obligations on any voice service provider whose program has failed

Questions and Comments?

Speak up now or email us any time:

- Josh Bercu: jbercu@ustelecom.org
- Jessica Thompson: jthompson@ustelecom.org
- David Frankel: traceback@ustelecom.org